ADVANCES I

Following on from Rich Merritt's article "Introduction to Fieldbus", describing the fundamentals of fieldbus technology, that appeared in the October/November edition of Process Industry Informer, and can be viewed on our website www.processindustryinformer.com this piece continues with further details of some of the awkward issues that fieldbus users might have to face:

hazardous area choices

integrating devices into systems from different manufacturers

redundancy and fault-tolerance

Hazardous Area Choices

One of the fundamentals of instrument engineers training in the last 30-some years is that 'intrinsic safety' is the best protection method for instrumentation, being somehow seen as the 'natural' method; conventional 4/20mA 2-wire instrumentation is low-powered and has zero & span adjustments which occasionally need access on the plant while the unit is 'live'. On both counts, intrinsically safe designs meet those criteria - the technique of intrinsic safety restricts the amount of available energy under normal (and certain reasonable fault) conditions, and remains safe even if the connecting wires are shorted accidentally in the hazardous location. I.S. instruments can be opened and adjusted as required, wiring connections made/unmade and even bare sensors exposed to continuously-present explosive hazards, such as inside closed vessels and pipes. These benefits were so strong that some of the disadvantages of intrinsic safety were brushed aside by many systems designers. For instance, I.S. loop design is much more complex than a standard 4/20mA loop and it is not unknown for designs to be produced which are perfectly safe but so energy-restricted that they are completely non-functional. (If you are approaching an external approval agency for I.S. certification, please remember that their responsibility is only to confirm that the instrument in its intended application is not going to cause an explosion - it is your responsibility to make sure that the instrument can actually be used!). External approval costs are high, especially if you would like to address a world-wide market, and users have to pick up that tab!

The use of fieldbus brings a particular problem; how to get enough power in an intrinsically safe segment to drive a lot of instruments on one pair of wires when it was already difficult to drive a single instrument. Using conventional barriers & isolators for fieldbus in the way that had become standard (trying to make the circuit safe for all Gas Groups and all Divisions/Zones) has led fieldbus designers to the '80mA & 4 devices' restriction (*see Rich's article of how that came about).

Engineering people love to remove complex problems, particularly if their own company is almost entirely focused on intrinsically safety designs. These supporters of intrinsic safety therefore worked tirelessly to bring us their solution for fieldbus - the Fieldbus Intrinsically Safe Concept (FISCO). After years of experimentation and consultation, FISCO now enables fieldbus users to have 115mA, instead of just 80mA. Using the 'rule-of-thumb' 20mA individual device load, FISCO segments in hydrogen risk areas (Group A/B for NEC, Gas Group IIC for IEC) can now have 4 devices and some cable! In practice, many FISCO devices are designed to take lower current (say, 12mA or 15mA) in order to still claim high numbers of devices per segment, but users should be aware that less current usually means less capability in the devices. Furthermore, the rules for using FISCO only allow 1000m (3250 ft) of cable in total and only 60m (195ft) spurs, reduced by about half compared to 'normal' fieldbus. FISCO also introduces a rarely mentioned drawback; the complexity of the FISCO electronic current-limiting design itself and the requirement to have multiple such circuits in series (current-limiting must still be available even if a circuit fails in an unsafe way) means that the overall MTTF of these units is much lower than users might expect (ask a FISCO power supply manufacturer for his MTTF calculations).

MooreHawke have a particularly innovative solution to the problem of intrinsically-safe fieldbus (CEP magazine "Best In Show" Award, ISA 2002) which was described in the previous article by *Rich. ROUTE-MASTER enables a full 350mA per segment and supports I.S. devices in all Gas Groups and all Divisions/Zones. ***See figure 1 for a graphical comparison between Entity segments, FISCO segments and Split-Architecture segments.***

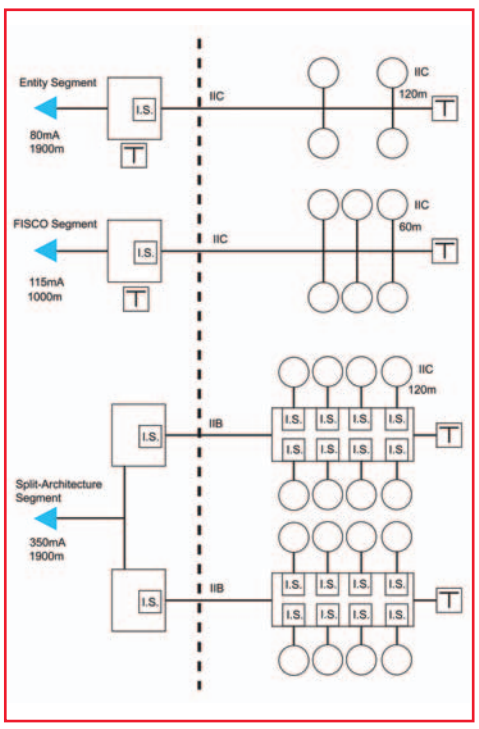

Figure 1

However, anyone casually looking at a fieldbus device or involved with fieldbus installation & commissioning will see that all adjustments to fieldbus devices are made through engineering workstations, laptops and PDA's. Fieldbus devices don't have external screws for zero/span potentiometers, nor need force-beam balancing or other on-line adjustments. It strikes me that the fundamental driver for intrinsic safety ('live' maintenance) has been and gone, leaving behind only the old problems (high cost, system complexity, required paperwork trail) plus a new one of low segment capacity (unless using ROUTE-MASTER).

Looking at the application slightly differently, users also want to be able to remove devices from fieldbus segments in hazardous areas without turning off the whole segment, and without going through complex disconnection procedures and mechanical interlocks, if they can be avoided. Non-incendive designs provide exactly that facility without overly restricting the total current in the segment, and so allow the standard rules for segment design to be used, typically based on 350mA per segment. More accurately, the individual spur connections at a suitable device coupler can be approved as *non-incendive energy-limited,* making them freely dis-connectable at that point (or at the device, if that is preferred) within Division 2 (Zone 2). The trunk connections are not approved in the same way and so cannot be disconnected 'live', but that isn't likely to be a real hardship; if anyone did for some reason want to disconnect a whole segment from a system, it is likely that the segment would be switched off first. An aside: FNICO (Fieldbus Non-Incendive Concept) is brought to you by the same people who were promoting FISCO. FNICO should be called FISCO-*lite* as it is based on FISCO with a slightly relaxed safety analysis compatible with Division 2 (Zone 2) use. FNICO allows 180mA or so (vendor dependent) but suffers from the same basic problems as FISCO. Its one salient feature over 'normal' non-incendive systems is that the FNICO trunk is energy-limited and so accessible in the hazardous area, but as mentioned above, this is not particularly useful and does not compensate for the other drawbacks (one being a virtual absence of FNICO-approved devices!).

The 'high-energy trunk' concept, as popularized by MooreHawke Fieldbus and others, meets all the criteria of real fieldbus systems; segment capacity is related to the power conditioner parameters (typically 350mA/24V) and cable lengths are the same as for non-hazardous segments (1900m/6175ft total, 120m/390ft spurs). The primary design tool for segment calculations becomes an application of Ohm's Law, just as in normal fieldbus design. Costs are controlled since non-incendive design is quite straight-forward and avoids the worst complexities of allowable fault analysis. Overall, MTTF's are the same as for normal fieldbus. Even field wiring is an opportunity for cost savings and conduit is no longer mandatory - Division 2 (Zone 2) wiring can be in open tray with PLTC/ITC (Power Limited Tray Cable/Instrument Tray Cable) or conventional armored cable. In short, non-incendive protection incorporating a high-energy trunk and energy-limited spurs is the new 'natural' technique for fieldbus in hazardous areas!

Hey, what about Division 1 (Zone 1) applications? How can users disconnect devices in those areas? A valid question and one covered in various ways. MooreHawke has a device coupler that has a magnetic interlock per spur - put the key in the slot, that spur is isolated and therefore accessible for re-wiring. Figure 2 shows the concept. This is great if IEC/AEx standards are being followed, since that particular device coupler can fit inside an Exe/AExe (increased safety) enclosure and spurs are fully accessible in Zone 1. For flameproof Division 1 applications, live de-mateable plug/socket

IN FIELDBUS

By: Mike O'Neill, Director, MooreHawke Fieldbus

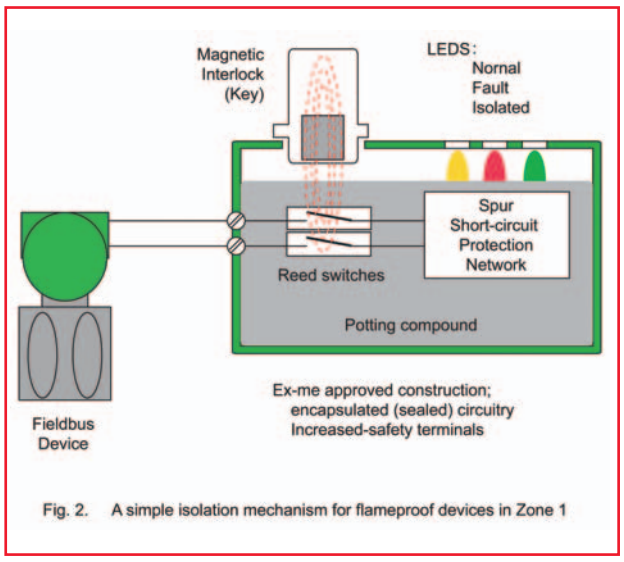

Fig. 2. A simple isolation mechanism for flameproof devices in Zone 1

combinations are available from many manufacturers, but I would question the cost effectiveness, particularly when attached to a flameproof junction box. If all else fails or an application demands live exposure in Division 1 or connection into Zone 0, then fieldbarriers can be used which allow intrinsically-safe spurs to be attached to the non-intrinsically safe trunk. Again, high unit cost inhibits universal use but since it is only individual spurs being made I.S., at least these designs avoid the major application restrictions of whole-segment I.S. packages. As most people now realize, the bulk of any plant with hazardous materials is Division 2 (Zone 2), and Division 1 (Zone 1) areas have to be small since they represent unacceptable environmental releases as well as product loss.

Integrating devices into systems from different manufacturers

In the old days of 4/20mA, the data available from every such instrument was the same; a signal representing the process variable and assumed to be in the range 0-100%. Each DCS used various hardware & software configurations to map these I/O points into internal software for processing. 'Intelligent' fieldbus devices have many, many parameters which may be used within any DCS, and so advanced methods are used to tell the DCS about the capabilities of those individual devices. HART devices were described by a text-based file called a Device Description (DD) and FF devices followed that same technology. PA devices had similar files called GSD files and the chief characteristic of both DD and GSD files was that they were text-based and limited in scope. The DCS had to be prepared to accept those files for those devices to operate within that system and some vendors even required the DD file to be modified in a particular way to be acceptable (described as a way that systems vendors could ensure that their users got only 'the best and most rigorously tested devices' to use, but also with other, less complimentary, descriptions). In order to make systems integration more open and the advanced features of devices more accessible to users, these device description files have been enhanced and improved to allow device manufacturers more flexibility in presenting their own data in ways which can be recognized by any DCS. These new files are called EDDs (Enhanced Device Descriptions) written in EDDL (Enhanced Device Description Language).

Naturally, in fieldbus there is always a competing technology and in the area of device interfacing, FDT/DTM is the name of the alternative. Since DDs were originally so limited and (almost) proprietary, the FDT/DTM concept emerged which allowed the DCS companies and the device manufacturers to concentrate on their individual core competencies. The device manufacturer wrote a Device Type Manager (DTM) to a defined specification which could then interface with any Field Device Tool (FDT) written by another party, usually but not necessarily a DCS vendor. A good analogy is that the DTM is the 'printer driver' and the DTM is that piece of the operating system that allows the user to use the features of the printer. This is great if everyone provided DTMs and everyone used the same operating system.

From the users perspective, he/she requires a software environment that is universal, unaffected by changes in base operating system and capable of supporting devices he already owns. EDDL is supported by FF, HART and Profibus as well as OPC and works with legacy FF/HART/PA devices. FDT/DTM will only support HART/FF/Profibus devices with FDT/DTM support built-in or which have been suitably converted post installation. FDT/DTM is based on various specific Microsoft Windows ActiveX components, which means DCS manufacturers or anyone else contemplating a HMI (Human Machine Interface) cannot use Linux or any other operating system. These components also change with successive versions of Windows and it is unclear who will revise FDT/DTM applications as a result of these changes. Finally, whereas all DCS manufacturers and device vendors have indicated support for EDDL, Emerson (US) and Siemens (Germany) which together form a not-insubstantial portion of the automation market, have pointedly refused to offer FDT/DTM as part of any devices from their respective portfolios. In summary, EDDL is the way forward.

Redundancy and fault-tolerance

One of the biggest and most long-standing issues with fieldbus for process control (FF and Profibus-PA) is the absence of meaningful redundancy. Users have always asked for fault-tolerance since they are being expected to commit many devices and control loops to one pair of cables. Redundancy is a part of practically every other cabled network, it seemed inconceivable that the field networks for process control could not provide that simple security measure. Vendors made every effort to convince users that redundancy of field cables was not required, even at the same time as they offered redundant cables within the control room and for systems interconnections. The provision of duplicated cables in a secure, protected environment while proposing that single cables in the 'wild woods' were quite adequate, seems to be a denial of obvious truths.

Technically, Manchester-encoded bus-powered (MBP) networks cannot operate in a ring without a further layer of software complication (collision detection and error checking) which would effectively reduce data transmission rates and seriously impair device numbers per segment. The search was on for a mechanism which could provide fault-tolerance without additional software overhead. Dr Hassan El-Sayed (ironically, based in Manchester, UK) invented a technology which made fault-tolerant MBP fieldbus a reality - the automatic terminator. Using this technology, the FF or Profibus-PA segment could be wired as a long U-shape, terminated at either end and driven by fieldbus-standard power conditioners. In the centre of the U-shape sits a fieldbus device coupler which can, on detection of a cable fault on either side, automatically terminate the remaining healthy leg and thus keep fieldbus communications alive. With additional refinements for cable open- and short-circuit protection and associated with physical layer diagnostics for fault detection and annunciation, truly fault-tolerant FF and Profibus-PA networks are now possible.

To the end-user, fault-tolerance means that overall plant availability can be significantly improved. A 'normal' redundant segment from most vendors comprises duplicated H1 cards, duplicated power conditioners and a single trunk twisted-pair cable to the field. The availability of such a segment can be calculated using published data and is of the order of 0.9998. Hardware failure of a cable on a process plant is not commonplace, but does have a finite risk (some cynics might suggest that accidental disconnection of cables by mistake is more likely). Howsoever brought about, if the consequences of that segment failure are severe, it seems foolhardy to ignore that risk. In fact, common practice in such circumstances to date is to alleviate that risk by avoiding fieldbus altogether, hardly a resounding cry of confidence in the technology. With fault-tolerant fieldbus, the hardware configuration per segment only increases by the addition of the second trunk cable. Both 'legs' of the U-shaped segment are continuously active to eliminate unfortunate surprises which can occur in master/standby redundancy designs, and no special software is required at the DCS to make it all work. The result is an improvement in segment availability to 0.99999998. Such a configuration need not be used on every segment on the plant, but can be easily incorporated for those segments carrying process-critical control loops. Indeed, it is now possible to design complete process automation networks with a properly graduated capability in respect of process significance: simplex segments for simple monitoring-only devices, duplex segments for regular control applications and fault-tolerant segments for critical loops. The overall result is actually an economic benefit, eliminating unnecessary hardware from simplex segments and allowing increased segment capacity even where control-in-the-field is being used. Saving money at both ends is a truly virtuous circle!

Note that fault-tolerance is an exercise in improving the availability of systems including fieldbus, not the generation of a fieldbus safety system. There is a very apt view that 'safety' and 'availability' are polar opposites, and a totally safe plant is one that completely unavailable (assuming that the plant is dangerous when it is operational and ignoring feedstock issues, etc). Fault-tolerance certainly helps in making systems safer, but designing SIL-compatible segments requires still more work. There is now TuV approval of an FF protocol for FF-SIS and Profibus has ProfiSAFE, but these both relate to the way in which field communications can be guaranteed and verified between the field devices and the shut-down system, called the black channel in safety circles. The fault-tolerant physical layer is the counterpart of the black channel safety-related software, and together they present a wonderful opportunity to really integrate operational and safety systems within one network.

All in all, fieldbus is an exciting technology. Application issues, which have irritated users for the last decade, now have solutions gradually coming into focus which will accelerate the uptake of fieldbus world-wide for the benefit of all. Users should feel more confident that a) fieldbus can be used in both non-hazardous areas and hazardous areas without undue restrictions, b) software describing device advanced performance characteristics will be easily interoperable between all DCS vendors and c) fieldbus segments can be as redundant and fault-tolerant as necessary to achieve the process operation objectives, within the same physical control system.

MooreHawke
Crawley
WEST SUSSEX

Can be contacted on

Tel: 01293 514488
Fax: 01293 536852
Mail to: moneill@miinet.com
Web: www.miinet.com/fieldbus